Towards a Process Assessment Model for IEC 80001-1

Silvana Togneri MacMahon, Fergal Mc Caffery and Frank Keenan
[1]Regulated Software Research Group, Department of Computing & Mathematics, Dundalk Institute of Technology & Lero, Dundalk Co. Louth, Ireland
{silvana.macmahon, fergal.mccaffery, frank.keenan}@dkit.ie

Keywords: IEC 80001-1, ISO/IEC 15504-2 – Process Assessment, Service Management, ISO/IEC 20000-1, TIPA, ITIL, Connected Health, Risk Management.

Abstract: Medical Devices are widely used in patient care for both diagnosis and treatment purposes. Typically, modern medical devices are intended to be networked at their point of use. The incorporation of medical devices opens up new opportunities and new vulnerabilities to patients and medical facilities. In 2010, the first standard to address the risks of incorporating a medical device into an IT network was published in the form of IEC 80001-1. Currently no method exists to allow responsible organisations - entities that operate and maintain a network that incorporates a medical device- to assess themselves against this standard. This paper discusses the how healthcare providers can be assessed against IEC 80001-1. This paper discusses the work carried out to date to develop a Process Reference Model and future work to allow this Process Reference Model to be extended to form a Process Assessment Model is also presented within this paper.

1 INTRODUCTION

Medical devices are designed and validated to ensure that they are safe for their intended use (Cooper et al., 2011). Whilst the device has been validated, the incorporation of the device into an IT network can introduce additional risks to the safety of the device. In order to address these risks, IEC 80001-1 - Application of risk management for IT networks incorporating medical devices (2010) was published outlining a lifecycle risk management approach to the incorporation of medical devices into an IT Network.. This paper describes how a Process Reference Model (PRM) has been developed and how this model will be extended to develop a Process Assessment Model (PAM) that can be used to assess against IEC 80001-1

2 IEC 80001-1 OVERVIEW

Medical devices are increasingly being designed to be incorporated into IT networks. Medical devices are subject to stringent regulations prescribed by the regulatory authorities of the region in which the device is to be marketed, such as the Food and Drug Administration (FDA) in the USA. While the FDA regulates medical devices from design to sale (and some aspects after sale), it cannot regulate the use or users of medical devices which includes how they are incorporated into an IT network (National Cybersecurity and Communications Integration Center, 2012).

IEC 80001-1 applies to responsible organisations, medical device manufacturers and providers of other IT technology. The standard *"represents a catalyst for a new level of IT and clinical technology cooperation to ensure network changes don't negatively impact biomedical systems"*(Cooper et al., 2011). The standard extends the definition of harm and in doing so identifies 3 main areas of risk by examining 3 key properties of the network – safety, effectiveness and (data & system) security IEC 80001-1 seeks to address these risks but how do organisations assess themselves against this standard? No method to assess against this standard currently exists. The goal of our research to date has been to develop a PRM (the first version of which has now been completed) and PAM (which will extend the PRM) to assess against IEC 80001-1.

3 PROCESS ASSESSMENT

In order to develop the assessment method for assessment against IEC 80001-1, a review of Process Assessment Standards was carried out. This review focused on ISO/IEC 15504-2:2003 Information technology - Process assessment (2003) which sets out the requirements for developing PRMs and PAMs and the requirements for performing an assessment and verifying conformity

of an assessment. ISO/IEC 15504-2 outlines requirements for performing an assessment from 2 dimensions – from the perspective of capability determination and from the perspective of process improvement. In order to perform an assessment which would be compliant with ISO/IEC 15504-2, a PRM and PAM would be required. The PAM is developed with reference to a PRM and extends the PRM with the addition of a measurement framework. Processes within the PRM and PAM are phrased in terms of their purpose and their outcomes. Additional guidance for the phrasing of processes is provided in ISO/IEC TR 24774 (2010).

3.1 Development of the PRM

In order to develop the assessment models to assess against IEC 80001-1 we performed a review of similar standards, focusing on Service Management Standards. Particular focus was given to ISO/IEC 20000-1:2011 Information technology - Service management which is a Service Management System (SMS) standard which specifies requirements for the service provider to take a lifecycle approach to Service Management and to plan, establish, implement, operate, monitor, review, maintain and improve an SMS (2011a) . It advocates an integrated process approach of Plan – Do – Check – Act. This means that the service is planned (Plan). Once operational (Do), the service being provided is checked against the original plan (Check) and on the basis of the results of checking the service against the plan, actions are taken to improve the service (Act).

The similarities between ISO/IEC 20000-1 and IEC 80001-1 are outlined in Annex D of IEC 80001-1. This annex outlines processes that are common to both e.g. Configuration Management. The annex also highlights areas where the terminology is different but the underlying role, process or document is similar as shown in Figure 1. Given the similarities between the 2 standards as outlined in Annex D of IEC 80001-1, we examined what assessment methods were available to assess against this SMS standard and investigated the development of these methods to assess if they could be used to develop a PRM and PAM for IEC 80001-1. Our investigation focused on the Tudor IT Service Management Process Assessment (TIPA) (Barafort et al., 2009) methodology which is used to assess against ISO/IEC 20000-1 and another service management standard – Information Technology Infrastructure Library (ITIL) (The Cabinet Office, 2011) and is compliant with the requirements for process assessment as described in ISO/IEC 15504-2.

3.2 TIPA Transformation Process

While ISO/IEC 15504-2 describes the requirements for the development of PRMs and PAMs, it does not give guidance on how to transform the input (in terms of the domain requirements) into the outputs (the PRM and PAM). To address this, the TIPA transformation process was developed by the Public Research Centre Henri Tudor in Luxembourg which is a goal oriented requirements engineering technique which produces PRMs and PAMs that are compliant with ISO/IEC 15504-2. The TIPA transformation process (Barafort et al., 2008) was used to develop a PAM to assess against ISO/IEC 20000-1 which is no longer maintained by CRP Henri Tudor but was used as an input to ISO/IEC 15504-8 (ISO/IEC, 2011b). ISO/IEC 15504-8 is the PAM now used to assess against ISO/IEC 20000-1. The TIPA transformation process was also used to develop a PRM and PAM to assess against ITIL. Table 1 outlines the steps within the TIPA transformation process which were used for the development of the PRM for IEC 80001-1. The TIPA transformation process was followed due to its use to develop both PRMs and PAMs to assess against Service Management standards, standards which are similar in approach to IEC 80001-1.

Table 1 – TIPA Transformation Process Steps

Description	PRM	PAM
Identify elementary requirements in a collection of requirements	X	
Organize, and structure the requirements	X	
Identify common purposes upon those requirements and organize them towards domain goals	X	
Identify and factorize outcomes from the common purposes and attach them to the related goals	X	
Group activities together under a practice and attach it to the related outcomes		X
Allocate each practice to a specific capability level		X
Phrase outcomes and process purpose	X	X
Phrase the Base Practices attached to Outcomes		X
Determine Work Products among the inputs and outputs of the practices		X

4 IEC 80001-1 PROCESS REFERENCE MODEL

Step 1 of the TIPA transformation process is to "*Identify elementary requirements in a collection of*

requirements". As the source of these requirements was IEC 80001-1, the standard was reviewed line by line and all potential requirements were identified and .were transferred into a requirements catalogue to allow us to begin to form the requirements into the first draft of the PRM. The original source of each requirement was noted and traceability was maintained throughout the process. A review of ISO/IEC 20000-4 was performed to be used as a template for the PRM.

Step 2 states that it is necessary to: *"Organize, and structure the requirements"*. The process groups within ISO/IEC 20000-4 were reviewed to understand if these groups could also be used to structure the requirements for IEC 80001-1. The structure was not deemed sufficient; however, given that both standards adopt a lifecycle approach, a decision was taken to maintain the use of the "Plan, Do, Check, Act approach. The approach taken to organise and structure the requirements, involved grouping requirements around topic areas as defined within the standard and followed the same structure as the standard.

Step 3 of the TIPA transformation process states *"Identify common purposes upon those requirements and organize them towards domain goals"*. As with step 2 above, it was found that the domain goals could be identified by following the structure of the standard and focusing upon how the topic areas were structured within the standard.

To complete the 4th step of the TIPA transformation process *("Identify and factorize outcomes from the common purposes and attach them to the related goals"*), the requirements were again reviewed to isolate outcomes from the common purposes and attach them to the related domain goals. Each identified purpose/domain goal was reviewed and an observable and assessable outcome was identified.

The identified purposes/domain goals would allow us to organise the identified purposes/goals into processes. The processes were then reviewed against the requirements as outlined in ISO/IEC TR 24774 as per step 7 of the TIPA transformation process. Step 7 of the TIPA transformation process states "*Phrase outcomes and process purpose*". At this stage the purpose and outcome elements of the processes have been completed so the final title and context elements were phrased as per the requirements.

4.1 IEC 80001-1 Process Groups

4.1.1 "Plan" – Process Groups

The "Plan" part of the lifecycle contains 2 process groups – Risk Management Policy Processes and Medical IT Network Risk Management Planning Processes. Risk Management Policy Processes contains a single process the purpose of which is to establish an overall risk management policy to determine acceptable risk levels and allow the responsible organisation to avoid unacceptable risks.

The Medical IT Network Risk Management Planning Processes contains 4 processes. The purpose of the Medical IT Network Planning process is to ensure that all risk management activities are adequately planned and are carried out in accordance with the established risk management policy. The Medical IT Network Documentation outlines the process for managing additional documentation provided by medical device manufacturers that describes the intended use of the device and gives instructions for the safe and effective use of the device. The Responsibility Agreements process looks in detail at when a responsibility agreement is required and the purpose of the process is to establish the responsibilities of medical device manufacturers and other IT providers with regard to risk management. The final process in the group is an umbrella process which sets out the responsibilities of the Medical IT Network Risk Manager in relation to the risk management process.

4.1.2 "Do" – Process Groups

The "Do" part of the lifecycle contains a single process group including the Medical IT Network Risk Management Process. The purpose of this process is to gather, analyse, assess and store information spanning planning, design, installation, device connection, configuration, use/operation, maintenance, and device decommissioning for lifecycle management of medical devices incorporated in IT-Networks. There are 3 further processes within the group. The purpose of the Risk Analysis & Evaluation process is to identify, analyse & evaluate risk related to the incorporation of Medical Device into IT Networks. The Risk Control process looks at how to control the risks which have been identified by the Risk Analysis & Evaluation process through the implementation of risk control measures until the residual risk is judged to be of an acceptable level. Once these measures have been implemented the Residual Risk process outlines how to assess residual risk and ensure that the risk control measures have been effective.

4.1.3 "Check" – Process Groups

The "Check" part of the lifecycle contains one process group: Live Network Risk Management Processes, with 2 processes. The Monitoring process allows the network to be monitored for emerging risks, effectiveness of risk control measures, and accuracy of original estimations of risk. The Event Management process ensures that adverse events during the operational phase are managed correctly.

4.1.4 "Act" – Process Groups

The "Act" part of the lifecycle contains one process group: Change/Release Management & Configuration Management which includes 3 processes. The purpose of the Change/Release & Configuration Management process is to ensure that a documented Change Release Process is in place and that risk management activities take place during the Change Release process. Acceptability of the change is based on the results of the risk management activities which are performed as part of the Change Release process. All changes to the system must be reflected in the current Configuration Management information held with regard to the network which is carried out as part of this process. The second process within this group is the Decision on how to apply Risk Management, the purpose is to ensure that a policy is in place to allow organisations to consider the nature of the change that is required to the medical IT network and to assess if the change should be carried out under a change permit or by initiating a medical IT network project. The final process within the group is concerned with risk management activities during the Go-Live phase of the lifecycle. The purpose of the process is to allow the responsible organisation to manage the transition of the IT network to the live environment and to allow the responsible organisation to manage the risk management activities associated with the Go-Live phase of the project.

6 FUTURE WORK

Future work in this area will focus on the extension of the PRM with the addition of a measurement framework to form the PAM. This PAM will then be validated within the international standards community and within a healthcare setting. An assessment method will also be developed.

ACKNOWLEDGEMENTS

This research is supported by the Science Foundation Ireland (SFI) Stokes Lectureship Programme, grant number 07/SK/I1299, the SFI Principal Investigator Programme, grant number 08/IN.1/I2030 (the funding of this project was awarded by Science Foundation Ireland under a co-funding initiative by the Irish Government and European Regional Development Fund), and supported in part by Lero - the Irish Software Engineering Research Centre (http://www.lero.ie) grant 10/CE/I1855.

ITIL® is a registered trade mark of the Cabinet Office. TIPA® is a Registered Trade Mark of the CRP Henri Tudor

REFERENCES

Barafort, B., Betry, V., Cortina, S., Picard, M., St Jean, M., Renault, A., Valdés, O. & Tudor, P. R. C. H. 2009. *ITSM Process Assessment Supporting ITIL : Using TIPA to Assess and Improve your Processes with ISO 15504 and Prepare for ISO 20000 Certification*, Zaltbommel, Netherlands, Van Haren.

Barafort, B., Renault, A., Picard, M. & Cortina, S. 2008. A transformation process for building PRMs and PAMs based on a collection of requirements – Example with ISO/IEC 20000. *SPICE* Nuremberg, Germany.

Cooper, T., David, Y. & Eagles, S. 2011. *Getting Started with IEC 80001: Essential Information for Healthcare Providers Managing Medical IT-Networks*, AAMI.

IEC 2010. IEC 80001-1 - Application of Risk Management for IT-Networks incorporating Medical Devices - Part 1: Roles, responsibilities and activities. Geneva, Switzerland: International Electrotechnical Commission.

ISO/IEC 2003. ISO/IEC 15504-2:2003 - Software engineering — Process assessment — Part 2: Performing an assessment. Geneva, Switzerland.

ISO/IEC 2010. ISO/IEC TR 24774:2010 - Systems and software engineering — Life cycle management — Guidelines for process description. Geneva, Switzerland.

ISO/IEC 2011a. ISO/IEC 20000-1:2011 - Information technology —Service management Part 1: Service management system requirements. Geneva, Switzerland.

ISO/IEC 2011b. ISO/IEC PDTR 15504-8 - Information technology -- Process assessment -- Part 8: An exemplar process assessment model for IT service management. Geneva, Switzerland.

National Cybersecurity and Communications Integration Center 2012. Attack Surface: Healthcare and Public Health Sector.

The Cabinet Office 2011. ITIL 2011 - Summary of Updates. Norfolk, England: Crown Copyright.